WIPI 환경에서의 XML 문서 암호화 시스템의 설계 및 구현

홍현우* · 이재승** · 문기영** · 김창수*** · 정회경*

*배재대학교 컴퓨터공학과 · **한국전자통신연구원 정보보호연구단 · ***청운대학교 인터넷학과

Design and Implementation of XML Encryption System based on WIPI Environment

Xian-Yu Hong* · Jae-Seung Lee** · Ki-Young Moon** · Cang-Su Kim*** · Hoe-Kyung Jung*

*Dept. of Computer Engineering, Paichai University · **Information Security Research Division, ETRI · ***Dept. of Internet, Chungwoon University

Email : *{hongxianyu · hkjung}@pcu.ac.kr, **{jasonlee · kymoon}@etri.re.kr, ***ddoja@chungwoon.ac.kr

요 약

최근에 모바일 환경에서도 PC 환경처럼 데이터 전송을 XML 문서를 이용하는 경우가 증가하고 있다. 그러나 모바일 환경에서 제한된 하드웨어 조건이나 현재 국내에서 활성화 되고 있는 모바일뱅킹 같은 서비스를 고려할 때 모바일 환경은 PC 환경보다 보다 높은 보안성을 요구하고 있다.

이에 본 논문에서는 모바일 환경에서 XML 문서의 암호화에 관련한 W3C 권고안의 요구사항에 맞추어 모바일 환경에서의 XML 문서 암호화 시스템을 설계 및 구현하였다. 본 시스템은 DES(Data Encryption Standard), Triple-DES, AES(Advanced Encryption Standard), SEED 및 RSA(Rivest Shamir Adleman) 알고리즘을 사용하였으며, 국내의 여러 무선 플랫폼이 공존하고 있는 현실을 고려하여 정부에서 추진하고 있는 무선 인터넷 표준인 WIPI 플랫폼에서 개발을 진행하였다.

ABSTRACT

Recently, Not only PC environment but also movile environment using XML for translating data. But the mobile delevopment is more limited but need highler security than PC environment Because there is some important service such as mobile banking.

In this paper, We development the system to encrypt and decrypt the XML data in order to protect data, And the system is observing the recommendation of the XML Encryption Syntax and Processing by W3C. When encrypting the data, We use the encryption algorithm DES, Triple-DES, AES, SEED and RSA. and consideration of the mobile environment Last, We test the system at WIPI environment.

키워드

모바일, 암호화, XML, WIPI

Ⅰ. 서 론

현재 휴대용 단말기는 무선 인터넷 통신기술과 단말기 제조기술의 발전으로 인해 다양한 서비스를 제공할 수 있는 종합적인 멀티미디어 기기로 발전하였다. 현재 휴대용 단말기는 음악서비스, 뉴스보기, GPS(Global Positioning System) 위치확인, 모바일게임, DMB(Digital Multimedia Broadcasting) 수신, Wibro(Wireless Broadband Internet)와 같은 여러 서비스를 제공하고 있다.

하지만 아직까지도 휴대용 단말기에서는 여러 플랫폼이 공존하여 단말기 제조업체들과 디지털 콘텐츠 개발업체들의 부담을 증가시켜 모바일 분야의 발전을 저해하고 있다. 이런 이동통신사간의 플랫폼의 차이로 인한 문제들을 해결하기 위하여 무선 인터넷 통합 플랫폼인 WIPI가 제안되었으며 국내 공식표준으로 채택되어 2.0까지 발표되었다.

특히 WIPI 개발이 아직도 진행 중이고 모바일 환경은 개인신상정보보호에 대하여 PC 환경보다 더욱 높은 보안성이 요구되고 있다. WIPI 환경에서 데이터 교환에 사용되는 XML 문서는 제3자에게 유출될 경우, 쉽게 정보가 노출되기 때문에 XML 문서에 대한 보안의 필요성이 증가

하고 있다

이에 본 논문에서는 모바일 환경에서 데이터 교환에 사용되고 있는 XML 문서를 암호화시킴으로서 중요한 데이터들의 보안성을 향상하는 암호화 시스템을 설계 및 구현하였다.

II. 관련연구

2.1 WIPI 플랫폼

WIPI는 단말기 OS나 Air 인터페이스에 독립적이며 기존의 WAP(Wireless Application Protocol)나 J2ME와도 호환되어 높은 호환성을 보장하고 있다. 또한 콘텐츠 개발을 지원하는 API를 지원하고 있으며 기존 플랫폼의 단점을 보완하고 차세대 서비스 기술을 반영하고 있다. 그림 1에 WIPI의 구성도를 보여주고 있다.

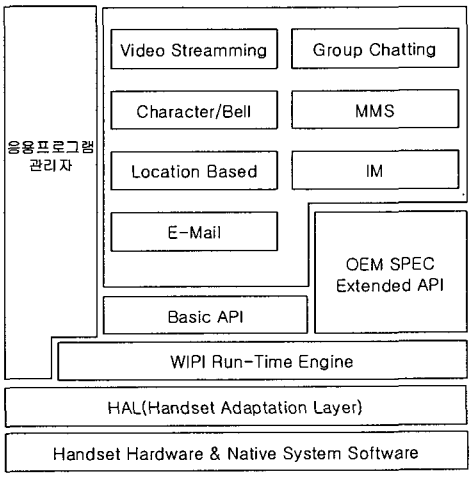

그림 4 WIPI 구성도

그림에서 WIPI는 HAL, Basic API, 응용프로그램 관리자, Dynamic Component 등으로 구성되었다.

1) HAL은 하드웨어에 대한 추상화를 실현하여 하드웨어 독립성을 지원하는 계층이다.

2) Basic API는 Java 및 C 언어로 구성되어 있는 응용프로그램 개발을 지원하고 있는 API 모음이며, C와 Java의 API와 기능면에서 동등한 기능을 제공한다.

3) 응용프로그램 관리자는 응용프로그램의 다운로드, 설치, 삭제를 관리한다.

4) Dynamic Component는 응용프로그램 관리자를 통하여 추가/갱신된 API 및 컴포넌트를 저장 및 관리한다.

2.2 XML 암호화

XML 문서는 현재 데이터 교환의 실질적인 표준으로 PC 환경 뿐만 아니라 모바일 환경에서도 널리 사용되고 있다. XML 문서 암호화는 문서의 전체 또는 일부분을 암호화할 수 있다. 특히 문서의 여러 부분을 암호화하는 경우에는 각각의 암호화 되는 부분에 서로 다른 암호화 알고리즘을 적용할 수 있는 특징이 있다. 또 이렇게 암호화된 문서는 XML 문서의 특징을 가지고 있어 XML 기반의 웹 서비스에도 자연스럽게 통합시킬 수 있는 이점이 있다[2].

W3C의 권고안에서는 암호화 유형을 XML 문서의 전체 암호화, 엘리먼트 암호화, 엘리먼트 데이터 암호화, 다중 암호화로 구분하였다.

그림 1은 W3C에서 제안한 XML 문서의 암호화 스키마 구조를 보여주고 있다.

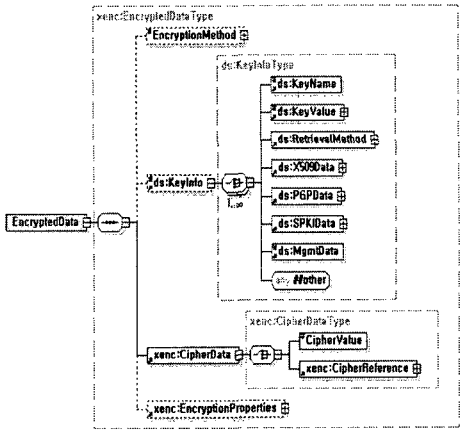

그림 2. XML 문서 암호화 스키마 구조

1. EncryptedData 요소(Element)는 XML 문서 암호화 구문에서 필수적인 핵심요소이며 암호화된 데이터를 대체하는 새로운 문서 루트처럼 사용된다.

2. EncryptedMethod 요소는 적용된 암호화 알고리즘을 기술하는 선택적인 요소이다. 이 요소가 생략된 경우는 수신자가 암호화 알고리즘을 이미 수신하여 알고 있어야 한다.

3. KeyInfo 요소는 복호화하기 위해 필요한 키 정보를 제공하고 있다. KeyInfo 요소는 하위 요소로 KeyValue 요소와 KeyName 요소를 포함한다. KeyValue 요소는 서명을 확인하고 데이터를 복호화 하는데 사용하는 공개키의 실제 값을 포함하며 요소로서 사용한 공개 키 알고리즘의 유형에 따라 RSAKeyValue 요소나, DSAKeyValue 등 요소를 포함할 수 있다. KeyName 요소는 키를 식별하기 위해 사용하는 문자열을 포함한다.

4. CipherData 요소는 암호화된 데이터를 제공하는 필수 요소이다. CipherData는 CipherValue 요소를 통하여 BASE64로 인코딩된 암호화된 데이터를 포함하거나 CipherReference 요소로 암호화된 데이터의 참조위치를 제공한다[3,4].

III. 시스템 설계

그림 2는 본 시스템의 전체 구성을 보여주고 있다.

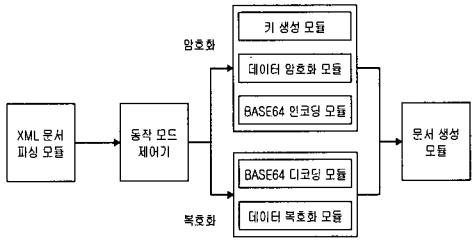

그림 3. 전체 시스템 구성도

시스템은 XML 문서를 수신한 다음 먼저 문서를 파싱하여 각 요소 정보를 분석한다. 만약 문서에 포함된 요소들 중에 EncryptedData 요소가 존재하지 않으면 시스템은 암호화 모드로 실행되고, EncryptedData 요소가 존재하면 복호화 모드로 실행된다.

3.1 암호화 모드

암호화 모드에서는 암호화하려는 데이터는 시스템 관리자가 지정할 수 있고 제공된 스키마에 따라 자동 설정도 가능하다. 또한 암호화에 사용될 블록 암호화 알고리즘도 시스템 관리자가 선택 가능하며 디폴트로 DES로 설정되어 있다.

시스템은 암호화키를 생성하고 다시 데이터 암호화를 진행한다. 암호화 된 데이터는 바이너리 데이터로서 XML 문서에 표현하기 위하여 다시 BASE64로 인코딩한다. 블록 암호화가 완료되면 시스템은 다시 RSA 알고리즘을 실행하여 블록 암호화에 사용한 키를 다시 RSA 공개키로 암호화 한다.

표 2는 본 시스템에서 사용한 암호화 알고리즘들의 정보를 보여주고 있다.

표 1. 본 시스템에서 사용한 암호화 알고리즘

	블록의 크기	키 크기	운영 모드
DES	64 비트	64 비트	CBC
Triple-DES	64 비트	128 비트	CBC
AES	128 비트	128 비트	CBC
SEED	128 비트	128 비트	CBC
RSA	DES/Triple-DES/AES/SEED의 키	512/1024/2048 비트	-

본 시스템에서는 블록 암호화 알고리즘으로 현재까지 많이 사용되고 있는 DES, DES의 단점을 보완한 Triple-DES, DES의 대체 표준인 AES, 그리고 국내 데이터 암호화 표준인 SEED를 사용하였으며 공개키 암호화 알고리즘으로는 RSA를 사용하였다. 이 중 블록 암호화는 권고안에 따라 CBC 방식을 사용하고 있다.

암호화가 완료된 데이터는 문서 생성 모듈에 전송된다. 문서 생성 모듈은 그림 1의 스키마구조를 참조하여 CipherData 요소의 하위 요소인 CipherValue에 암호화 된 데이터를 포함시키고, KeyValue 요소의 하위 요소인 RSAKeyValue 요소에 RSA 공개키를 포함시켜 EncryptedData 요소로 원 문서의 암호화될 요소를 대체한다.

3.2 복호화 모드

복호화 모드에서는 EncryptedData 요소로부터 암호화된 데이터 값, 암호화에 사용한 알고리즘, 암호화된 키값 등의 정보를 추출하여 암복호화 모듈에 전송한다. 데이터 암복호화 모듈은 먼저 RSA 개인키를 사용하여 암호화된 키를 복호화한다. 다음 암호화된 데이터를 BASE64로 디코딩하고 복호화를 진행하고 생성된 정보를 문서 생성 모듈에 전송한다. 문서생성 모듈에서는 복호화된 데이터로 EncryptedData 요소를 대체하여 원 XML 문서로 변환한다.

IV. 시스템 구현 및 고찰

4.1 시스템 구현

본 구현은 IBM-PC 호환 컴퓨터(Pentium 4 3.0G)와Windows XP Professional Service Pack 2의 운영체제 환경에서 표준 C언어를 사용하여 개발 하였으며, XML 문서의 파싱을 위해 사용한 DOM 파서인 xmlParser4Etri.lib를 사용하였다. 테스트 환경은 SKT사의 SCH-W210 단말에서 시뮬레이션을 진행하였다.

시스템 구현에서는 XML 문서 암호화 시스템을 모바일 단말기와 PC 환경의 서버에 탑재하여 전자상거래 시나리오를 구축하여 모바일 단말기에서 XML 문서를 암호화 하여 PC에 전송한 다음 다시 PC에서 복호화를 진행하였다. 아래 그림은 시스템의 실행을 보여주고 있다.

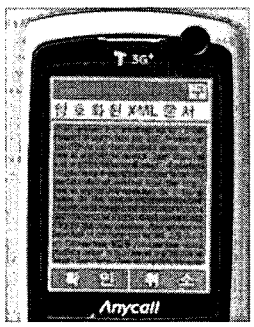

그림 4. 모바일 말기에서
XML 문서 암호화

모바일 단말기의 화면을 보면 XML 문서가 그

림 1의 스키마 구조에 따라 암호화가 성공한 것을 확인할 수 있다. 암호화된 문서를 다시 복호화하면 그림 2의 스키마를 따르는 결제문서로 회복된 것을 확인할 수 있다.

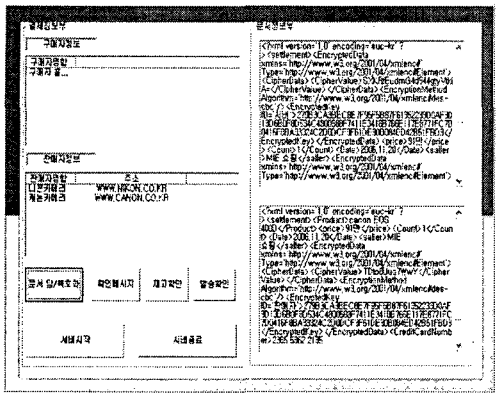

그림 5 PC에서 XML 문서 복호화

위의 그림 5는 모바일 단말로부터 전송받은 암호화된 XML 문서를 복호화한 결과를 보여준다.

4.2 고찰

본 시스템의 장점은 WIPI 플랫폼의 표준화 작업과 같이 진행되어 보안원천기술을 확보하였다는 것이며, XML 문서 암호화에 관련된 권고안에 따라 문서내의 여러 부분을 독립적으로 다중 암호화하였다는 것을 들수 있다.

본 시스템의 또 하나의 장점은 현재 진행 중인 XML 문서 권고안에 맞추어 대칭키 암호화 알고리즘과 공개키 암호화 알고리즘을 적용하여 XML 문서의 보안을 강화한데 있다. 그러나 RSA 알고리즘 같은 경우는 보안성이 높고, 대칭키 암호화에 비해 키 관리가 용이하지만 실행속도가 느리다.

표 2는 본 시스템에서 암호화키에 RSA 알고리즘을 적용할 때 소모되는 시간을 20회 측정한 평균시간이다.

현재 512 비트의 RSA 키는 보안성이 떨어져 실제 응용에서는 1024 비트 이상의 키를 사용할 것을 제안하고 있다. 표 2를 보면 생성하는 RSA 알고리즘의 키 길이가 2048 비트일 때 시스템에서의 시간소모가 너무 많다는 단점이 있다. 현재 시스템에서의 실행속도와 보안성을 모두 고려할 때 1024 비트의 RSA 키가 가장 적합한 것으로 사료된다.

표 2. 시스템 암호화 실행속도

	DES	Triple-DES	AES	SEED
RSA 512 비트	2 초	4 초	3 초	3 초
RSA 1024 비트	4 초	6 초	5 초	5 초
RSA 2048 비트	17 초	19 초	18 초	18 초

V. 결 론

현재 국내에서는 모바일 단말기상의 WIPI 플랫폼의 표준화가 진행됨에 따라, 점점 더 많은 콘텐츠 제공업체들이 WIPI 관련 개발에 관심을 가지고 사업영역을 확대하고 있다. 또한 WIPI를 기반으로 한 모바일상의 여러 서비스가 빠른 속도로 발전되어 소비자에게 이용되고 있다. 하지만 WIPI 표준화는 아직 진행 중이기 때문에 WIPI 환경에서 악성 코드나 해킹 프로그램에 의해 데이터 유출을 대비하는 암호화 프로그램이 필요하다.

이에 본 논문에서는 WIPI 환경에서의 데이터 교환에 주로 사용되는 XML 문서에서 필요한 데이터를 암호화하여 데이터 유출에 의한 피해를 대비하기 위한 연구를 진행하였다. 현재 W3C에서 진행 중인 XML 문서 암호화에 관한 관련 권고안을 연구하여 이를 바탕으로 데이터 보안에서 많이 사용되던 DES, Triple-DES, AES, SEED, RSA 등의 알고리즘으로 암호화 시스템을 설계 및 구현하였다.

본 시스템은 표준화 작업이 진행중인 WIPI 플랫폼을 대상으로 개발되었으며 WIPI 플랫폼에서 처음으로 개발된 보안 시스템으로 원천기술의 확보에 의의가 있다.

참고문헌

[1] "Cryptography and Network Security", William Stallings, 2005

[2] "Secure XML: The New Syntax for Signatures and Encryption", Donald E. Eastlake III, 2003

[3] "XML Encryption Syntax and Processing", Takeshi Imamura, Blair Dillaway, Ed Simon, W3C Recommendation, 2002

[4] "확장성 생성언어 암호 구문과 처리", 한국정보통신기술협회, TTAS.KO-10.0185, 2005

[5] "모바일 표준 플랫폼 규격 V2.0.1", 한국 무선인터넷 표준화 포럼, 2004